

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Claims 1 – 17 Canceled.

18. (Currently Amended) An improved method for encryption including multiplication over a finite field, the improvement comprising:
obtaining the result of multiplication over a finite field using a primitive power and log table comprising 2 rows ~~The method of claim 16~~, wherein obtaining the result of multiplication over a the finite field comprises obtaining the result of multiplication over a Galois field(2^8) performed in the MixColumns transformation and in the InvMixColumns transformation of the AES algorithm, using a 2 by 256 primitive power and log table, comprising the steps of:
- looking up logs of terms being multiplied over the Galois field(2^8);
 - summing the logs to obtain a sum; and
 - looking up the anti-log of the sum.

Claims 19 – 21 Canceled.